Quantum Hacking on Continuous-Variable Quantum Key Distribution System using a Wavelength Attack

Jing-Zheng Huang,[1] Christian Weedbrook,[2] Zhen-Qiang Yin*,[1] Shuang Wang†,[1] Hong-Wei Li,[1] Wei Chen,[1] Guang-Can Guo,[1] and Zheng-Fu Han[1]

[1]*Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China*
[2]*Center for Quantum Information and Quantum Control, Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, M5S 3G4, Canada*

(Dated: February 4, 2013)

The security proofs of continuous-variable quantum key distribution are based on the assumptions that the eavesdropper can neither act on the local oscillator nor control Bob's beam splitter. These assumptions may be invalid in practice due to potential imperfections in the implementations of such protocols. In this paper, we consider the problem of transmitting the local oscillator in a public channel and propose a wavelength attack which can allow the eavesdropper to control the intensity transmission of Bob's beam splitter by switching the wavelength of the input light. Specifically we target continuous-variable quantum key distribution systems that use the heterodyne detection protocol using either direct or reverse reconciliation. Our attack is proved to be feasible and renders all of the final key shared between the legitimate parties insecure, even if they have monitored the intensity of the local oscillator. To prevent our attack on commercial systems, a simple wavelength filter should be added before performing the monitoring detection.

PACS numbers:

I. INTRODUCTION

Quantum key distribution (QKD) enables two distant partners, Alice and Bob, to share common secret keys in the presence of an eavesdropper, Eve [1, 2]. In theory, the unconditional security of QKD protocol is guaranteed based on the laws of physics, in particular the no-cloning theorem. But in practice, the key components of practical QKD systems have imperfections that do not fulfill the assumptions of ideal devices in theoretical security proofs. In discrete-variable QKD, the imperfect devices such as single photon detectors, phase modulators, Faraday mirrors and fiber beam splitters, open security loopholes to Eve and lead to various types of attacks [3–14].

Continuous-variable (CV) QKD [15] has developed immensely over the past decade [16] to the point that there are companies selling commercially available systems [17, 18]. Even so, CV-QKD is potentially vulnerable to such idealization-to-practical problems that plague its discrete variable counterpart. In the CV-QKD protocols, Alice encodes the key information onto the quadratures, $\hat{X}$ and $\hat{P}$, on a bunch of coherent states and sends them onto Bob. Bob measures one or both quadratures by performing homodyne [19] or heterodyne detection [20] on the signal with a relatively strong local oscillator (LO). Finally, they perform direct or reverse reconciliation and privacy amplification process to distill a common secret key [1, 15]. In practice, it is extremely difficult for Bob to generate the LO with the same initial polarization and phase to Alice's signal. Therefore, Alice prepares both the signal and LO, and send them to Bob in the same optical fiber channel at the same time to avoid the large drifts of the relative polarization and phase [21]. However, this implementation leaves a security loophole open for Eve.

In Ref. [22], the authors proposed an equal-amplitude attack. To perform this attack, Eve first intercepts the signal and LO, and measures both of the quadratures by performing heterodyne detection on them. According to her measurement results, she reproduces two weak squeezed states which have the same intensity level to the signal, and sends them onto Bob. Bob treats these two fake states as signal and LO, and performs detections on them as usual. But now the detection is neither homodyne nor heterodyne detection, therefore Eve is able to make the extra noise of Bob's measurement much lower than the shot noise level. As a result, the total deviation between Bob's measurement and Alice's preparation is lower than the tolerable threshold derived from the theoretical security proofs [23, 24]. Hence Alice and Bob can not discover the presence of Eve.

In order to prevent this attack without modifying the original measurement setup, Bob needs to monitor the total intensity or the LO intensity [22]. We note that in this attack, Eve is assumed to be unable to control the beam splitters of Bob. But in one of our recent studies [13], we found that it is possible for Eve to control the outputs of fiber beam splitters by utilizing its wavelength dependent property [25–27]. Importantly, such wavelength dependent properties can be found in commercial CV-QKD systems [17, 18]. Making use of this loophole, we propose a new wavelength attack on a practical CV-QKD system using heterodyne detection protocol [20]. By using this attack Eve can in principle achieve all of the secret key without being discovered, even if Bob has monitored the total intensity or the LO intensity. Such an attack has practical and commercial consequences.

In the security analysis of CV-QKD protocols with direct (reverse) reconciliation, $V_{A|B}(V_{B|A})$, Alice (Bob)'s conditional variance of Bob (Alice), has the similar status as the quantum bit error rate (QBER) in the discrete-variable QKD

*yinzheqi@mail.ustc.edu.cn
†wsycy@mail.ustc.edu.cn

protocols. To show that the hidden Eve would not be discovered in our attack, our method is proving that the upper bound of $V_{A|B}$ ($V_{B|A}$) under our wavelength attack is always lower than the maximum value allowed by the secret key rate formula [20, 24].

This paper is organized as follows. In Section II, we first review the heterodyne protocol and the wavelength-dependent property of certain fiber beam splitters, then we propose a wavelength attack scheme on an all-fiber CV-QKD system using heterodyne protocol in Section III. We prove the feasibility of this wavelength attack in Section IV, and finally conclude in Section V.

II. PRELIMINARY

A. Heterodyne detection protocol

In the heterodyne protocol [20], Alice first prepares a displaced vacuum state that will be sent to Bob. This is realized by choosing two real numbers X_A and P_A from a Gaussian distribution of variance V_A and zero mean. The whole ensemble of coherent states Alice will send to Bob is given by the thermal state with variance $V = V_A + 1$. Bob receives this coherent state and simultaneously measures both the amplitude and phase quadratures of the state using heterodyne detection. After repeating this process many times, they finally extract a binary secret key by using either direct reconciliation [28] or reverse reconciliation algorithm [20]. A typical CV-QKD system using heterodyne protocol can be realized by the schematic shown in Fig. 1. In this scheme, time and polarization multiplexing are used so that the signal and LO can be transmitted in the same channel without interfering. To avoid the equal-amplitude attack [22], Bob uses a $1:99$ beam splitter(not depicted in the figure) behind the polarization beam splitter to monitor the LO intensity.

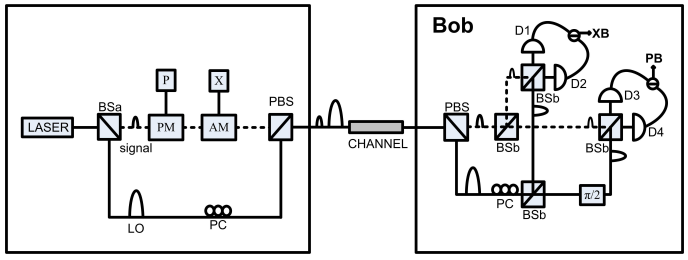

FIG. 1: The schematic diagram of heterodyne detection protocol. BSa: $1/99$ beam splitter; BSb: 50/50 beam splitter; PM: phase modulator; AM: amplitude modulator; PBS: polarization beam splitter; PC: polarization controller. Alice generates coherent light pulses by a 1550 nm laser diode, then separates them into a weak signal and a strong LO by a $1/99$ beam splitter. The signal is then modulated randomly following the centered Gaussian distribution in both quadratures, by using phase and amplitude modulators. The signal and LO are separated in time and modulated into orthogonal polarizations by the PBS before begin inserted into the channel.

To perform the heterodyne detection, Bob uses the photodetector to convert the photons into a photocurrent $\hat{i}$. Here $\hat{i}$ and the photon number $\hat{n}$ are related by $\hat{i} = q\hat{n} = q\hat{a}^\dagger\hat{a}$, where $\hat{a}$ and $\hat{a}^\dagger$ are the annihilation and creation operators of the light state, and q is a suitable constant [29]. The extra quantum noise $\delta\hat{\alpha}_v$ is unavoidable in Bob's measurement results when he uses heterodyne detection due to the unused port of the $50:50$ beam splitter. To show this, let us first describe the signal and LO by operators $\hat{\alpha}_s$ and $\hat{\alpha}_{LO}$, respectively. These operators can be broken up into two contributions [30]: the mean values of the amplitude α as well as the quantum noise fluctuations $\delta\alpha$. The operators can be written as

$$\begin{aligned}\hat{\alpha}_s &= \alpha_s + \delta\hat{\alpha}_s,\\ \hat{\alpha}_{LO} &= \alpha_{LO} + \delta\hat{\alpha}_{LO}.\end{aligned} \tag{1}$$

where α_s and α_{LO} are complex numbers and we assume that the amplitude of the LO is much larger than the signal, i.e., $|\alpha_{LO}| \gg |\alpha_s|$, and $\delta\hat{\alpha}_s$ and $\delta\hat{\alpha}_{LO}$ are the fluctuations of the signal and LO, respectively.

The photocurrents read by the four photo-detectors can be written as follows

$$\begin{aligned}\hat{i}_1 &= q(\alpha_{LO}^* + \delta\hat{\alpha}_{LO}^{'\dagger} + \alpha_s^* + \delta\hat{\alpha}_s^{'\dagger})\times\\ &\quad(\alpha_{LO} + \delta\hat{\alpha}'_{LO} + \alpha_s + \delta\hat{\alpha}'_s)/4,\\ \hat{i}_2 &= q(\alpha_{LO}^* + \delta\hat{\alpha}_{LO}^{'\dagger} - \alpha_s^* - \delta\hat{\alpha}_s^{'\dagger})\times\\ &\quad(\alpha_{LO} + \delta\hat{\alpha}'_{LO} - \alpha_s - \delta\hat{\alpha}'_s)/4,\\ \hat{i}_3 &= q[e^{-i\frac{\pi}{2}}(\alpha_{LO}^* + \delta\hat{\alpha}_{LO}^{'\dagger}) + \alpha_s^* + \delta\hat{\alpha}_s^{'\dagger}]\times\\ &\quad[e^{i\frac{\pi}{2}}(\alpha_{LO} + \delta\hat{\alpha}'_{LO}) + \alpha_s + \delta\hat{\alpha}'_s]/4,\\ \hat{i}_4 &= q[e^{-i\frac{\pi}{2}}(\alpha_{LO}^* + \delta\hat{\alpha}_{LO}^{'\dagger}) - \alpha_s^* - \delta\hat{\alpha}_s^{'\dagger}]\times\\ &\quad[e^{i\frac{\pi}{2}}(\alpha_{LO} + \delta\hat{\alpha}'_{LO}) - \alpha_s - \delta\hat{\alpha}'_s]/4.\end{aligned} \tag{2}$$

Here we have absorbed the vacuum noise terms $\delta\hat{\alpha}_v$ into the terms $\delta\hat{\alpha}'$. For simplicity, let us assume that α_{LO} is a real number. To derive the quadratures $\hat{X}$ and $\hat{P}$, the difference of the two photocurrents should be measured

$$\begin{aligned}\delta\hat{i}_x &= i_1 - i_2\\ &\approx q(\alpha_{LO}\alpha_s^* + \alpha_{LO}\alpha_s + \alpha_{LO}\delta\hat{\alpha}_s^{'\dagger} + \alpha_{LO}\delta\hat{\alpha}'_s)/2\\ &= \tfrac{q\alpha_{LO}}{2}(\alpha_s + \alpha_s^* + \delta\hat{\alpha}'_s + \delta\hat{\alpha}_s^{'\dagger})\\ &= \tfrac{q\alpha_{LO}}{2}(X + \delta\hat{X}'),\\ &\to \hat{X}_B = \tfrac{2}{q\alpha_{LO}}\delta\hat{i}_x = X + \delta\hat{X}',\\ \delta\hat{i}_p &= i_3 - i_4\\ &\approx q(i\alpha_{LO}\alpha_s^* - i\alpha_{LO}\alpha_s + i\alpha_{LO}\delta\hat{\alpha}_s^{'\dagger} - i\alpha_{LO}\delta\hat{\alpha}'_s)/2\\ &= \tfrac{q\alpha_{LO}}{2}(\tfrac{\alpha_s - \alpha_s^*}{i} + \tfrac{\delta\hat{\alpha}'_s - \delta\hat{\alpha}_s^{'\dagger}}{i})\\ &= \tfrac{q\alpha_{LO}}{2}(P + \delta\hat{P}'),\\ &\to \hat{P}_B = \tfrac{2}{q\alpha_{LO}}\delta\hat{i}_p = P + \delta\hat{P}',\end{aligned} \tag{3}$$

where $X \equiv \alpha_s + \alpha_s^*$ and $P \equiv -i(\alpha_s - \alpha_s^*)$ are the exact quadratures that Bob wants to measure, $\delta\hat{X}' \equiv (\delta\hat{\alpha}_s + \delta\hat{\alpha}_s^\dagger) + (\delta\hat{\alpha}_v + \delta\hat{\alpha}_v^\dagger) = \delta\hat{X} + \delta\hat{X}_v$ and $\delta\hat{P}' \equiv -i(\delta\hat{\alpha}_s - \delta\hat{\alpha}_s^\dagger) - i(\delta\hat{\alpha}_v - \delta\hat{\alpha}_v^\dagger) = \delta P + \delta P_v$ are the quantum noises entering into Bob's measurement. Several terms have been neglected above according to the fact that $|\alpha_{LO}| \gg |\alpha_s|$. $\delta\hat{X}$ and $\delta\hat{P}$ satisfy the canonical commutation relation $[\delta\hat{X}, \delta\hat{P}] = 2i$, therefore

the Heisenberg uncertainty relation $\langle(\delta\hat{X})^2\rangle\langle(\delta\hat{P})^2\rangle = 1$ is derivable [29].

Under the condition that Eve cannot act on the LO (a common assumption in the security proofs [1]), it is only when the excess noise reaches two times the shot-noise level that Eve can perform an intercept-resend attack on the channel [31]. It is due to the fact that Eve will introduce vacuum noise by using heterodyne detection and consequently, suffer the quantum fluctuations when she reproduces the signal state in a simple intercept-resend attack.

B. Wavelength-dependent fiber beam splitter

In Ref. [13], we studied the wavelength-dependent property of the fiber beam splitter which is made by the fused biconical taper technology [25]. The fused biconical taper beam splitter is made by closing two or more bare optical fibers, fusing them in a high temperature environment and drawing their two ends at the same time. Subsequently, a specific biconic tapered waveguide structure can be formed in the heating area. The fused biconical taper beam splitter is widely use in the fiber QKD systems because of the feature of low insertion loss, good directivity and low cost. However, intensity transmission of the fused biconical taper beam splitter is wavelength-dependent, and most types of fused biconical taper beam splitters work only in a limited range of wavelengths (limited bandwidths), where the intensity transmission of the beam splitter can be defined as $T \equiv I_{port1}/(I_{port1} + I_{port2})$, where I_{port1} (I_{port2}) is output light intensity from beam splitter's output port 1 (2). Typical coupling ratio at the center wavelength provides optimal performance, but the intensity transmission varies periodically with wavelength changes. The relationship between wavelength λ and the intensity transmission T by using the coupling model is given in Ref. [26, 27]:

$$T = F^2 \sin^2\left(\frac{C\lambda^{5/2}w}{F}\right) \equiv T(\lambda). \tag{4}$$

where F^2 is the fraction of power coupled, $C \cdot \lambda^{5/2}$ is the coupling coefficient, and w is the heat source width.

III. WAVELENGTH ATTACK ON A CV-QKD SYSTEM USING HETERODYNE PROTOCOL

The basic idea of the wavelength attack is shown in Fig. 2. Eve intercepts the coherent states sent by Alice. She makes heterodyne measurement of the signal using the LO to achieve the quadrature values X_E and P_E. After that, Eve generates and re-sends two coherent states: a fake signal state $|\alpha_s'\rangle$ and a fake LO state $|\alpha_{LO}'\rangle$. Different from the previous intercept-resend attack, these two fake states have different wavelengthes, denoted as λ_1 (for $|\alpha_s'\rangle$) and λ_2 (for $|\alpha_{LO}'\rangle$). According to Eq. (4), the performance of Bob's beam splitter is dependent on the wavelength of the incoming light. Therefore the fake signal with wavelength λ_1, the transmission

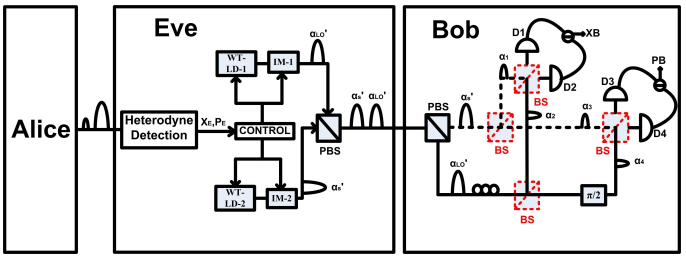

FIG. 2: The schematic diagram of the wavelength attack scheme. WT-LD: the wavelength tunable laser diode; IM: the intensity modulator; BS: 50/50 beam splitter. The WT-LD and IM are used in producing fake coherent states with the specific wavelength and amplitude set by the controller. The red (dotted) beam splitters are the ones controlled by Eve. The red beam splitter on the left has transmission T_1, while the red beam splitter down the bottom has transmission T_2.

of Bob's beam splitter is determined by the function $T(\lambda_1)$ which is defined in Eq. (4). Similarly, the intensity transmission of Bob's beam splitter to the fake LO state is determined by $T(\lambda_2)$. In other words, Eve can control Bob's beam splitter by tuning the wavelength of her fake states.

With the help of the wavelength tunable laser diodes and intensity modulators, the wavelength and amplitude of these fake states are carefully chosen to satisfy the following conditions

$$\begin{aligned}
&(i) \quad |\alpha_s'|^2 + |\alpha_{LO}'|^2 = |\alpha_s|^2 + |\alpha_{LO}|^2,\\
&(ii) \quad (1-T_2')|\alpha_{LO}'|^2 = 0.01|\alpha_{LO}|^2,\\
&(iii) \quad (1-T_1)(1-2T_1)|\alpha_s'|^2 + (1-T_2)(2T_2-1)|\alpha_{LO}'|^2\\
&\qquad = \frac{\sqrt{\eta}X_E|\alpha_{LO}|}{2},\\
&(iv) \quad T_1(1-2T_1)|\alpha_s'|^2 + T_2(2T_2-1)|\alpha_{LO}'|^2\\
&\qquad = \frac{\sqrt{\eta}P_E|\alpha_{LO}|}{2},
\end{aligned} \tag{5}$$

where $T_1 \equiv T(\lambda_1) \in [0,1], T_2 \equiv T(\lambda_2) \in [0,1], T_2' \equiv T'(\lambda_2) \in [0,1]$. Here η is the channel transmission efficiency, $|\alpha_s|$ and $|\alpha_{LO}|$ are the amplitudes of the original signal and the LO, respectively, $|\alpha_s'|$ and $|\alpha_{LO}'|$ are the amplitudes of the fake signal and the fake LO, T_2' is the intensity transmissions of Bob's $1:99$ beam splitter (for monitoring the LO light intensity) when the fake LO enters it. Condition (i) ensures the total intensity is unchanged and condition (ii) makes sure the method of monitoring the LO intensity is also invalid to Eve. Here we assume that Bob uses a $1:99$ beam splitter to split the LO light. Because the 1:99 beam splitter is also wavelength-dependent if it is made by the fused biconical taper technology, its intensity transmission can be determined by a function similar to Eq. (4), which is denoted by $T'(\lambda) \simeq F'^2 \sin^2(\frac{C'\lambda^{5/2}w'}{F'})$.

As Bob measures the quadratures $\hat{X}_B$ and $\hat{P}_B$ by performing heterodyne detection on the fake signal and the fake LO, conditions (iii) and (iv) make Bob's measurement results coincide with the ones attained by Eve. To see explicitly where these relations come from, see Eqs. (A5) and (A6) in the Appendix. Notice that the fake signal and the fake LO have different wavelengths, and hence, no interference occurs in this detection. The effect of this on the measurement detection

is that we no longer have heterodyne detection outputs but rather outputs that are proportional to Eve's measurements. Therefore, the photocurrents recorded by the photo-detectors consist of parts from the signal and the LO. We are going to prove in Section IV that the extra noise introduced by Bob's measurement is much lower than the shot-noise level, therefore the total noise can be kept under the alarm threshold. In other words, Eve can safely achieve the key information without being discovered by Alice or Bob.

Finally, we note that if there were no limits to T_1, T_2 and T_2', i.e., $\{T_1, T_2, T_2'\} \in (-\infty, \infty)$, the four parameters $\lambda_1, \lambda_2, |\alpha_s'|$ and $|\alpha_{LO}'|$ are sufficient to achieve conditions (i)-(iv). But as we must require $T \in [0, 1]$, we note that conditions (iii) and (iv) may not always be satisfied. However, by numerical simulation we find that the probability of failing condition (iii) or (iv) is extremely close to zero thanks to the fact that $|\alpha_{LO}|^2 \gg V_E$. To explain this let's look at an example. Let us assume that Alice chooses $|\alpha_{LO}|^2 = 10^8$ and $V = 11$ and the parameters of Eq. (4) are taken from [13]. To make our conclusion more convincing, we narrow the range of T_1 and T_2 to be $[0.1, 0.9]$, and restrict both $|\alpha_s'|^2$ and $|\alpha_{LO}'|^2$ to be larger than 10^3. The simulation result shows that conditions (iii) and (iv) can always be satisfied if $|X_E|, |P_E| \leq 50$. Notice that the distribution of X_E and P_E is a Gaussian distribution with variance of $V_E \simeq V_A$, it is easy to derive that the probability of $|X_E| > 50$ or $|P_E| > 50$ equals $\mathrm{erfc}(\frac{50}{\sqrt{22}}) \simeq 0$, where $\mathrm{erfc(x)} \equiv \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-x^2} dx$ is the error integral function.

Moreover, Eve can do even better by adding more wavelengths to the fake states. For example, the fake signal and fake LO can both be composed of two coherent states and in such a case Eve becomes more powerful because she has more control. By using the same method in Section IV B, the feasibility of this modified scheme can also be proved.

IV. FEASIBILITY ANALYSIS

To analyze the feasible of the wavelength attack, we first note that the following assumptions should be satisfied:

(1) This attack is restricted to an all-fiber coherent-state CV-QKD using heterodyne protocol.

(2) All of Bob's beam splitters have the same wavelength dependent property, i.e., their intensity transmissions are all determined by Eq.(4) with the same parameters. This function and the detection efficiencies of Bob's detectors are both known by Eve. Here we assume that the detection efficiencies are wavelength independent for simplicity. In practice, Eve can simply absorb the differences into the light amplitudes modulated by her and the final results are unchanged.

(3) Eve has the ability to replace the quantum channel with a noiseless fiber, and her detectors have high efficiency and negligible excess noise.

In the heterodyne protocol, the lower bound of the secret key rates for Heisenberg-limited individual attack in direct reconciliation and reverse reconciliation are given, respectively, by [32]

$$K^{DR} \geq \log_2 \frac{(1+\chi)[1+\eta(V+\chi)]}{(1+\chi V)[1+\eta(1+\chi)]}, \tag{6}$$

$$K^{RR} \geq \log_2 \frac{V+\eta(1+\chi V)}{\eta(1+\chi V)[1+\eta(1+\chi)]}, \tag{7}$$

where $\chi \equiv (1-\eta)/\eta + \epsilon$ is the total added noise referred to the input, $(1-\eta)/\eta$ stands for the loss-induced vacuum noise, ϵ is the excess noise above the shot noise level. Note that we use the 'Heisenberg-limited attack' rather than the optimal attack [24, 32] as such an attack upper bounds Eve's information thereby emphasizing our wavelength attack which can even beat such a stringent attack. To make the secret key rate positive, we require that

$$\chi < \chi_{max}^{DR} = \frac{\sqrt{4\eta^2+1}-1}{2\eta}, \tag{8}$$

with $\frac{2}{3} < \eta < 1$ for direct reconciliation or

$$\chi < \chi_{max}^{RR} = \frac{\sqrt{(\frac{4}{\eta^2}+1)V^2-2V+1}-V-1}{2V}, \tag{9}$$

with $0 < \eta < 1$ for reverse reconciliation, should be satisfied.

Another important parameter in the security proof is Alice's (Bob's) conditional variance of Bob's (Alice's) measurement $V_{A|B}$ ($V_{B|A}$) in direct reconciliation (reverse reconciliation), which can be thought of as the uncertainty in Alice's (Bob's) estimates of Bob's (Alice's) quadrature measurement result. In the CV-QKD, Alice and Bob use $V_{A|B}$ ($V_{B|A}$) to estimate the shot noise and modulation imperfections [21]. $V_{A|B}$ is defined (where both quadratures are symmetrized) as

$$V_{A|B} = V_A - \frac{\langle X_A \hat{X}_B \rangle^2}{\langle \hat{X}_B^2 \rangle}, \tag{10}$$

and similarly, we have $V_{B|A}$ defined as

$$V_{B|A} = V_B - \frac{\langle X_A \hat{X}_B \rangle^2}{\langle X_A^2 \rangle}. \tag{11}$$

We now proceed to consider the conditional variance values for the two cases: the usual eavesdropping attack and a wavelength attack.

A. Eve's Typical Attack

Even in typical eavesdropping attack, $V_{A|B}$ ($V_{B|A}$) is at the shot noise level because of the vacuum noises introduced by Alice's modulation, the channel loss and Bob's heterodyne measurement. The evolution of the quadrature value, with channel noise, from a real value X_A chosen by Alice to the measurement result $\hat{X}_B$ achieved by Bob is listed as follows (we write down the quadrature $\hat{X}$ only since the other quadrature $\hat{P}$ can be presented in the similar way)

$$\begin{aligned} X_A &\rightarrow \hat{X}_A = X_A + \hat{N}_A \\ &\rightarrow \hat{X}_{B'} = \sqrt{\eta}\hat{X}_A + \sqrt{1-\eta}\hat{X}_N \\ &\rightarrow \hat{X}_B = \tfrac{1}{\sqrt{2}}(\sqrt{\eta}\hat{X}_A + \sqrt{1-\eta}\hat{X}_N + \hat{N}_B) \\ &= \tfrac{1}{\sqrt{2}}(\sqrt{\eta}X_A + \sqrt{\eta}\hat{N}_A + \sqrt{1-\eta}\hat{X}_N + \hat{N}_B), \end{aligned} \tag{12}$$

where $\hat{X}_N$ is the quadrature of the inserted vacuum state due to channel loss, and $\hat{N}_B$ is the vacuum noise introduced by the heterodyne detection.

1. $V_{A|B}^{normal}$ *in direct reconciliation*

In direct reconciliation, Alice's conditional variance of Bob's measurement in the absence of Eve, which we will denote as $V_{B|A}^{normal}$, can be calculated as follows

$$V_{A|B}^{normal} = \frac{(V-1)[\eta(\chi+1)+1]}{\eta(V+\chi)+1}. \quad (13)$$

where $V_N \equiv \langle \hat{X}_N^2 \rangle$ is the variance of the channel noise, which can be related to χ by $V_N = \eta\chi/(1-\eta)$. Combining Eq. (13) with Eq. (8), we can find that for the sake of deriving a positive secret key rate, the upper bound of $V_{A|B}^{normal}$ yields

$$V_{A|B}^{max} = \frac{(V-1)(\sqrt{4\eta^2+1}+2\eta+1)}{\sqrt{4\eta^2+1}+2\eta V+1}. \quad (14)$$

In other words, if $V_{A|B}$ is smaller than this threshold, the heterodyne protocol in direct reconciliation is considered to be secure. Hence we prove our attack feasible by showing that Eve can make $V_{A|B} < V_{A|B}^{max}$ when she is performing the wavelength attack.

2. $V_{B|A}^{normal}$ *in reverse reconciliation*

In reverse reconciliation, Alice's conditional variance of Bob's measurement in the absence of Eve, which we denote as $V_{B|A}^{normal}$, can be calculated as follows

$$V_{B|A}^{normal} = \frac{1}{2}[\eta(1+\chi)+1]. \quad (15)$$

Combining with Eq. (9), the upper bound of $V_{B|A}^{normal}$ is derived to be

$$V_{B|A}^{max} = \frac{\sqrt{(4+\eta^2)V^2-2\eta^2V+\eta^2}+(\eta+2)V-\eta}{4V}. \quad (16)$$

In other words, if $V_{B|A}$ is smaller than this threshold, the heterodyne protocol in reverse reconciliation is considered to be secure. Hence we prove our attack feasible by showing that Eve can make $V_{B|A} < V_{B|A}^{max}$ when she is performing the wavelength attack.

B. Eve's Wavelength Attack

When Eve performs the wavelength attack, the evolution of the quadratures from X_A to $\hat{X}_B$ are written as follows

$$\begin{aligned} X_A \to \hat{X}_A &= X_A + \hat{N}_A \\ \to \hat{X}_E &= \frac{1}{\sqrt{2}}(\hat{X}_A + \hat{N}_E) \\ \to \hat{X}_B &= \sqrt{\eta}\hat{X}_E + \hat{N}_B, \end{aligned} \quad (17)$$

where $\hat{N}_E$ represents the vacuum noise in Eve's heterodyne detection, whose variance is normalized to 1. The variance of each of the terms is given by: $V_E = \frac{1}{2}(V+1)$ and $V_B = \eta V_E + V_{NB}$. Here V_{NB} can then be considered as Eve's conditional variance of Bob's measurement result. In Appendix A, we derive the value of V_{NB} and show that it is smaller than $10^{-2}\eta(V+1)$. For practical purposes, let us set $V = 11$, therefore $V_{NB} \sim \frac{\eta}{10}$.

1. $V_{A|B}^{attack}$ *in direct reconciliation*

According to the definition of $V_{A|B}$ in Eq. (10), the value of $V_{A|B}^{attack}$ can be computed as follows

$$V_{A|B}^{attack} = \frac{2(V_{NB}+\eta)(V-1)}{2V_{NB}+\eta(V+1)}. \quad (18)$$

Combining with Eq. (A9) and the discussions above, we can estimate that the value of $V_{A|B}^{attack}$ is not larger than 2.1. As shown in Fig. 3 (where we set $V = 11$ and $\epsilon = 0.01$ [24]), $V_{A|B}^{attack}$ is always lower than $V_{A|B}^{max}$, so that Alice and Bob can never discover the eavesdropper under this attack. Besides, one should notice that $V_{A|B}^{attack}$ is always lower than the normal level, therefore Eve should increase the deviations on purpose to make $V_{A|B}^{attack}$ close to $V_{A|B}^{normal}$ in order to avoid suspicion.

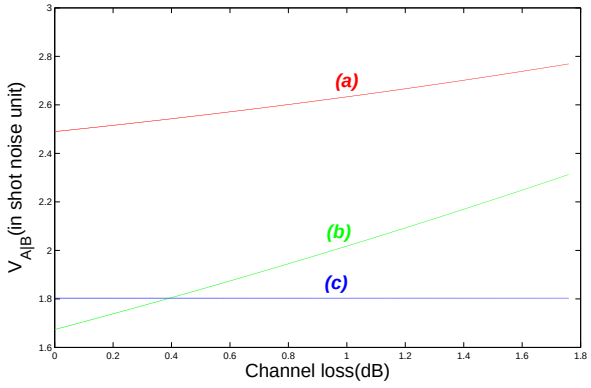

FIG. 3: In direct reconciliation, the relation between the channel loss and the conditional variance $V_{A|B}$ in three cases: (a) the maximum tolerable value $V_{A|B}^{max}$. (b) the value of $V_{A|B}^{normal}$ and (c) the value of $V_{A|B}^{attack}$. See main text for details. The curves are plotted for experimentally realistic values, $V = 11$ and $\epsilon = 0.01$. We can see that $V_{A|B}^{attack}$ is always lower than $V_{A|B}^{max}$ and lower than $V_{A|B}^{normal}$ when the channel loss is larger than 0.4 dB at which point the key between Alice and Bob is no longer secure.

2. $V_{B|A}^{attack}$ *in reverse reconciliation*

In reverse reconciliation, using Eq. (11) with Eq. (17), the value of $V_{B|A}^{attack}$ can be computed as

$$V_{B|A}^{attack} = \eta + V_{NB}. \quad (19)$$

Combining with Eq. (A9) and the discussions above, we can estimate that the value of $V_{B|A}^{attack}$ is never larger than 1.1η. As shown in Fig. 4 (where again we have set $V = 11$ and $\epsilon = 0.01$), it is always lower than the value of $V_{B|A}^{max}$ so that Alice and Bob can never discover the eavesdropper under such an attack. Besides, one should notice that $V_{B|A}^{attack}$ is lower than the $V_{B|A}^{normal}$ when the channel loss is larger than 0.41 dB. Hence, Eve should increase the deviations to make $V_{A|B}^{attack}$ close to $V_{A|B}^{normal}$ in order to avoid suspicions.

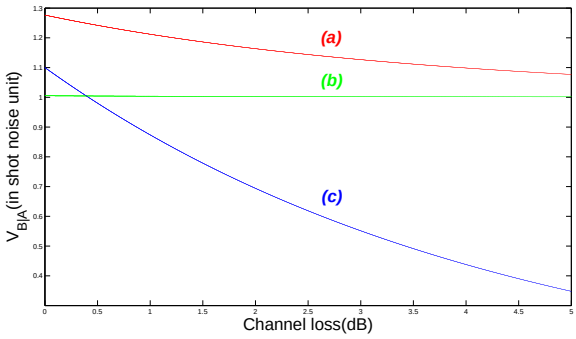

FIG. 4: In reverse reconciliation, the relation between the channel loss and the conditional variance $V_{B|A}$ in three cases: (a) the maximum tolerable value $V_{B|A}^{max}$. (b) the value of $V_{B|A}^{normal}$ and (c) the value of $V_{B|A}^{attack}$. See main text for details. The curves are plotted for experimentally realistic values, $V = 11$ and $\epsilon = 0.01$. We can see that $V_{B|A}^{attack}$ is always lower than $V_{B|A}^{max}$ and lower than $V_{B|A}^{normal}$ when the channel loss is greater than 0.4 dB, again leading to an insecure key.

V. DISCUSSIONS AND CONCLUSION

There are several points about the wavelength attack that should be remarked:

1. As shown in Fig. 4, $V_{B|A}^{attack} < 1$ when $\eta < 0.91$. It is impossible when the protocol works normally, therefore Eve should add extra noise on her measurement result to increase $V_{B|A}^{attack}$. So that perfect heterodyne detection is not necessary for Eve. In other words, assumption (3) listed in Section IV can be compromised.

2. It is a little surprising that $I_{AE} > I_{AB}$ and $I_{BE} > I_{BA}$. That is because V_{NB} can be made much lower then the shot noise, which means Eve guesses Alice's (Bob's) measurement result more precisely than Bob (Alice) does. Therefore Eve can make the whole key shared by Alice and Bob insecure.

3. To be aware of our attack, Bob should not only add a $1:99$ beam splitter to monitor the intensity, but also add a wavelength filter before the monitoring detector.

As we have discussed in Section III, Eve can do better by using more than two wavelengths to produce the fake states. The feasibility analysis for this kind of attack is similar to the one we have derived in Section IV B. One can still use Eqs. (18) and (19) but the value of V_{NB} should be re-estimated. For the four-wavelength scheme which is depicted at the end of Section III, one can easily find that the result $V_{NB} \sim \frac{\eta}{10}$ holds, therefore the conclusions in Section IV B 1 and Section IV B 2 remain the same.

Finally, we note that a commercial CV-QKD system, as sold by [17], currently uses a wavelength-dependent beam splitter. Although, it does not fall into the regime studied in this paper because it uses homodyne detection rather than heterodyne detection. However, our results show that if one were going to use heterodyne detection with a commercial QKD unit, then the precautions mentioned here would need to be taken. Furthermore, possible quantum hacking opportunities with homodyne detection and wavelength-dependent beam splitters warrant further investigation.

In conclusion, we have proposed a new type of realistic quantum hacking attack, namely the wavelength attack, on continuous-variable QKD systems using heterodyne detection. If Alice and Bob don't take the necessary precautions for such an attack, the final secret key is in principle, totally insecure as Eve can obtain all the information about the final key. This is different from the equal-amplitude attack proposed in Ref. [22] as in the wavelength attack, Eve has the ability to control Bob's beam splitter and therefore the suggestion of testing the total intensity in Ref. [22] would not prevent such an attack from occurring. To close such a loophole in practical CV-QKD systems, it is simply enough for Bob to add a wavelength filter before his detection.

A. Acknowledgement

This work was supported by the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200), National Natural Science Foundation of China (Grants No. 60921091 and No. 61101137). C. W. acknowledges support from the Ontario postdoctoral fellowship program, CQIQC postdoctoral fellowship program, CIFAR, Canada Research Chair program, NSERC, and QuantumWorks.

Appendix A: Derivation of V_{NB}

To derive V_{NB}, let us start from the generation of Eve's fake states. As we have described in Section III, Eve generates the fake signal state and the fake LO state according to her measurement results and sends them to Bob. These fake states can be described by the following operators

$$\begin{aligned} \hat{\alpha}'_s &= \alpha'_s + \delta\hat{a}'_s, \\ \hat{\alpha}'_{LO} &= \alpha'_{LO} + \delta\hat{a}'_{LO}. \end{aligned} \tag{A1}$$

Where complex numbers α'_s and α'_{LO} are the amplitudes and $\delta\hat{a}'_s$ and $\delta\hat{a}'_{LO}$ represent the fluctuations of the amplitudes as discussed in Section II A. Similarly, $\langle(\delta\hat{X}'_k)^2\rangle = \langle(\delta\hat{P}'_k)^2\rangle =$

1, where $\delta\hat{X}_k = \delta\hat{a}'_k + \delta\hat{a}_k^{'\dagger}$ and $\delta\hat{P}_k = -i(\delta\hat{a}'_k - \delta\hat{a}_k^{'\dagger})$, k = s, LO.

Bob performs heterodyne detection on these fake states. According to Eq. (4), Bob's beam splitter has different intensity transmissions for $\hat{\alpha}'_s$ and $\hat{\alpha}'_{LO}$ because of their different wavelengths, denoted as T_1 and T_2. After passing the first set of beam splitters, $\hat{\alpha}'_s$ is separated into $\hat{\alpha}_1$ and $\hat{\alpha}_3$, while $\hat{\alpha}'_{LO}$ is separated into $\hat{\alpha}_2$ and $\hat{\alpha}_4$ (cf. Fig. 2), which can be expressed as follows

$$\begin{aligned}
\hat{\alpha}_1 &= \sqrt{1-T_1}\hat{\alpha}'_s + \sqrt{T_1}\delta\hat{a}_{v1},\\
\hat{\alpha}_2 &= \sqrt{1-T_2}\hat{\alpha}'_{LO} + \sqrt{T_2}\delta\hat{a}_{v2},\\
\hat{\alpha}_3 &= \sqrt{T_1}\hat{\alpha}'_s - \sqrt{1-T_1}\delta\hat{a}_{v1},\\
\hat{\alpha}_4 &= e^{i\frac{\pi}{2}}(\sqrt{T_2}\hat{\alpha}'_{LO} - \sqrt{1-T_2}\delta\hat{a}_{v2}),
\end{aligned} \tag{A2}$$

where $\delta\hat{a}_{v1}$, $\delta\hat{a}_{v2}$ are the vacuum noises that interfere with the fake signal and the fake LO, respectively, at Bob's beam splitter. To simplify the symbols, let us define $\delta\hat{\alpha}'_1 \equiv \sqrt{1-T_1}\delta\hat{a}'_s + \sqrt{T_1}\delta\hat{\alpha}_{v1}$, $\delta\hat{\alpha}'_2 \equiv \sqrt{1-T_2}\delta\hat{a}'_{LO} + \sqrt{T_2}\delta\hat{\alpha}_{v2}$, $\delta\hat{\alpha}'_3 \equiv \sqrt{T_1}\delta\hat{a}'_s - \sqrt{1-T_1}\delta\hat{\alpha}_{v1}$ and $\delta\hat{\alpha}'_4 \equiv \sqrt{T_2}\delta\hat{a}'_{LO} - \sqrt{1-T_2}\delta\hat{\alpha}_{v2}$. Furthermore, we define the quadratures of $\delta\hat{\alpha}'_k$ by $\delta\hat{X}_k = \delta\hat{\alpha}'_k + \delta\hat{\alpha}_k^{'\dagger}$ and $\delta\hat{P}_k = -i(\delta\hat{\alpha}'_k - \delta\hat{\alpha}_k^{'\dagger})$ where $k = 1, 2, 3, 4$. Finally, after combining at the second set of beam splitters, the electromagnetic fields arrive at the four detectors can be written as

$$\begin{aligned}
\hat{b}_1 &= \sqrt{1-T_1}\hat{\alpha}_1 + \sqrt{T_2}\hat{\alpha}_2,\\
\hat{b}_2 &= \sqrt{T_1}\hat{\alpha}_1 - \sqrt{1-T_2}\hat{\alpha}_2,\\
\hat{b}_3 &= \sqrt{1-T_1}\hat{\alpha}_3 + \sqrt{T_2}\hat{\alpha}_4,\\
\hat{b}_4 &= \sqrt{T_1}\hat{\alpha}_3 - \sqrt{1-T_2}\hat{\alpha}_4.
\end{aligned} \tag{A3}$$

where the photocurrents are given by $\hat{i}_k = q\hat{b}_k^\dagger\hat{b}_k$. Bob's quadrature measurement results are then derived from the difference in photocurrents, using the method in Section II A. Firstly, for detectors $D1$ and $D2$, we have

$$\begin{aligned}
\hat{i}_x &= \hat{i}_1 - \hat{i}_2\\
&= q(\hat{b}_1^\dagger\hat{b}_1 - \hat{b}_2^\dagger\hat{b}_2)\\
&= q[(1-2T_1)[(1-T_1)|\alpha'_s|^2 + \sqrt{1-T_1}(\alpha'^*_s\delta\hat{\alpha}'_1 + \alpha'_s\delta\hat{\alpha}_1'^\dagger) + \delta\hat{\alpha}_1^\dagger\delta\hat{\alpha}_1]\\
&+\sqrt{(1-T_1)T_2}[\sqrt{(1-T_1)(1-T_2)}(\alpha'^*_s\alpha'_{LO} + \alpha'_s\alpha^*_{LO}) + \sqrt{1-T_1}(\alpha'^*_s\delta\hat{\alpha}'_2 + \alpha'_s\delta\hat{\alpha}_2^\dagger)\\
&+\sqrt{1-T_2}(\alpha'_{LO}\delta\hat{\alpha}_1'^\dagger + \alpha'^*_{LO}\hat{\alpha}'_1) + \delta\hat{\alpha}_1'^\dagger\delta\hat{\alpha}'_2 + \delta\hat{\alpha}'_1\delta\hat{\alpha}_2'^\dagger]\\
&-\sqrt{(1-T_2)T_1}[\sqrt{(1-T_1)(1-T_2)}(\alpha'^*_s\alpha'_{LO} + \alpha'_s\alpha^*_{LO}) + \sqrt{1-T_1}(\alpha'^*_s\delta\hat{\alpha}'_2\\
&+\alpha'_s\delta\hat{\alpha}_2^\dagger) + \sqrt{1-T_2}(\alpha'_{LO}\delta\hat{\alpha}_1'^\dagger + \alpha'^*_{LO}\hat{\alpha}'_1) + \delta\hat{\alpha}_1'^\dagger\delta\hat{\alpha}'_2 + \delta\hat{\alpha}'_1\delta\hat{\alpha}_2'^\dagger]\\
&+(2T_2-1)[(1-T_2)|\alpha'_{LO}|^2 + \sqrt{1-T_2}(\alpha'^*_{LO}\delta\hat{\alpha}'_2 + \alpha'_{LO}\delta\hat{\alpha}_2'^\dagger) + \delta\hat{\alpha}_2^\dagger\delta\hat{\alpha}_2].
\end{aligned} \tag{A4}$$

Note that $\hat{\alpha}'_{LO}$ and $\hat{\alpha}'_s$ have different frequencies, therefore any terms not containing the product of the same frequencies vanish during the measurement. The remaining terms compose the measurement result of $\hat{i}_x$

$$\begin{aligned}
\hat{i}_x &= q[(1-T_1)(1-2T_1)|\alpha'_s|^2 + (1-2T_1)\sqrt{1-T_1}(\alpha'^*_s\delta\hat{\alpha}'_1 + \alpha'_s\delta\hat{\alpha}_1'^\dagger)\\
&+(1-T_2)(2T_2-1)|\alpha'_{LO}|^2 + (2T_2-1)\sqrt{1-T_2}(\alpha'^*_{LO}\delta\hat{\alpha}'_2 + \alpha'_{LO}\delta\hat{\alpha}_2'^\dagger)].
\end{aligned} \tag{A5}$$

Similarly, we get the measurement result of $\hat{i}_p$ as:

$$\begin{aligned}
\hat{i}_p &= \hat{i}_3 - \hat{i}_4 = q(\hat{b}_3^\dagger\hat{b}_3 - \hat{b}_4^\dagger\hat{b}_4)\\
&= q[T_1(1-2T_1)|\alpha'_s|^2 + (1-2T_1)\sqrt{T_1}(\alpha'^*_s\delta\hat{\alpha}'_3 + \alpha'_s\delta\hat{\alpha}_3'^\dagger)\\
&\quad + T_2(2T_2-1)|\alpha'_{LO}|^2 + (2T_2-1)\sqrt{T_2}(\alpha'^*_{LO}\delta\hat{\alpha}'_4 + \alpha'_{LO}\delta\hat{\alpha}_4'^\dagger)].
\end{aligned} \tag{A6}$$

Notice that the squared modulus terms in the last two equations are what helped us derive the set of conditions in Eq. (5). The measurement results corresponding to Bob's quadratures $\hat{X}_B$ and $\hat{P}_B$ are then calculated using Eq. (3):

$$\begin{aligned}
\hat{X}_B &= \tfrac{2\hat{i}_x}{q|\alpha_{LO}|}\\
&= \tfrac{2[(1-T_1)(1-2T_1)|\alpha'_s|^2 + (1-T_2)(2T_2-1)|\alpha'_{LO}|^2]}{|\alpha_{LO}|}\\
&+\tfrac{2[(1-2T_1)\sqrt{1-T_1}(\alpha'^*_s\delta\hat{\alpha}'_1 + \alpha'_s\delta\hat{\alpha}_1'^\dagger) + (2T_2-1)\sqrt{1-T_2}(\alpha'^*_{LO}\delta\hat{\alpha}'_2 + \alpha'_{LO}\delta\hat{\alpha}_2'^\dagger)]}{|\alpha_{LO}|}\\
&= \sqrt{\eta}X_E + \hat{X}_{NB},\\
\hat{P}_B &= \tfrac{2\hat{i}_x}{q|\alpha_{LO}|}\\
&= \tfrac{2[T_1(1-2T_1)|\alpha'_s|^2 + T_2(2T_2-1)|\alpha'_{LO}|^2]}{|\alpha_{LO}|}\\
&+\tfrac{2[(1-2T_1)\sqrt{T_1}(\alpha'^*_s\delta\hat{\alpha}'_3 + \alpha'_s\delta\hat{\alpha}_3'^\dagger) + (2T_2-1)\sqrt{T_2}(\alpha'^*_{LO}\delta\hat{\alpha}'_4 + \alpha'_{LO}\delta\hat{\alpha}_4'^\dagger)]}{|\alpha_{LO}|}\\
&= \sqrt{\eta}P_E + \hat{P}_{NB}.
\end{aligned} \tag{A7}$$

where we have used conditions (iii) and (iv) from Eq. (5). Let α'_{LO} and α'_s be real, we then get the following inequalities:

$$\begin{aligned}
\hat{X}_{NB} &= \frac{2[(1-2T_1)\sqrt{1-T_1}(\alpha'_s\delta\hat{\alpha}'_1+\alpha'_s\delta\hat{\alpha}'^{\dagger}_1)+(2T_2-1)\sqrt{1-T_2}(\alpha'_{LO}\delta\hat{\alpha}'_2+\alpha'_{LO}\delta\hat{\alpha}'^{\dagger}_2)]}{|\alpha_{LO}|} \\
&= \frac{2[(1-T_1)(1-2T_1)\alpha'^2_s\frac{\delta\hat{\alpha}'_1+\delta\hat{\alpha}'^{\dagger}_1}{\alpha'_s\sqrt{1-T_1}}+(1-T_2)(2T_2-1)\alpha'^2_{LO}\frac{\delta\hat{\alpha}'_2+\delta\hat{\alpha}'^{\dagger}_2}{\alpha'_{LO}\sqrt{1-T_2}}]}{|\alpha_{LO}|} \\
&< \frac{2[(1-T_1)(1-2T_1)\alpha'^2_s\delta\hat{X}'_1+(1-T_2)(2T_2-1)\alpha'^2_{LO}\delta\hat{X}'_2]}{|\alpha_{LO}|}\cdot\frac{1}{\alpha\sqrt{1-T_{max}}}, \\
\hat{P}_{NB} &= \frac{2[T_1(1-2T_1)(\alpha'_s\delta\hat{\alpha}'_3+\alpha'_s\delta\hat{\alpha}'^{\dagger}_3)+T_2(2T_2-1)(\alpha'_{LO}\delta\hat{\alpha}'_2+\alpha'_{LO}\delta\hat{\alpha}'^{\dagger}_4)]}{|\alpha_{LO}|} \\
&= \frac{2[T_1(1-2T_1)\alpha'^2_s\frac{\delta\hat{\alpha}'_3+\delta\hat{\alpha}'^{\dagger}_3}{\alpha'_s\sqrt{T_1}}+T_2(2T_2-1)\alpha'^2_{LO}\frac{\delta\hat{\alpha}'_4+\delta\hat{\alpha}'^{\dagger}_4}{\alpha'_{LO}\sqrt{T_2}}]}{|\alpha_{LO}|} \\
&< \frac{2[T_1(1-2T_1)\alpha'^2_s\delta\hat{X}'_3+T_2(2T_2-1)\alpha'^2_{LO}\delta\hat{X}'_4]}{|\alpha_{LO}|}\cdot\frac{1}{\alpha\sqrt{T_{min}}},
\end{aligned} \tag{A8}$$

where $\alpha^2 = \min(|\alpha'_s|^2, |\alpha'_{LO}|^2)$, $T_{max} = \max(T_1, T_2)$, $T_{min} = \min(T_1, T_2)$ and $\delta\hat{X}'_1 \equiv \delta\hat{\alpha}'_1 + \delta\hat{\alpha}'^{\dagger}_1$ and similar to $\delta\hat{X}'_{2-4}$. Therefore,

$$\begin{aligned}
V_{NB,x} &= \langle(\hat{X}_{NB})^2\rangle < \tfrac{\eta\langle X_E^2\rangle}{\alpha^2(1-T_{\max})}\cdot\max(\langle\delta\hat{X}'^2_1\rangle, \langle\delta\hat{X}'^2_2\rangle) \\
&= \tfrac{\eta(V+1)}{\alpha^2(1-T_{\max})}, \\
V_{NB,p} &= \langle(\hat{P}_{NB})^2\rangle < \tfrac{\eta\langle P_E^2\rangle}{\alpha^2 T_{\min}}\cdot\max(\langle\delta\hat{X}'^2_3\rangle, \langle\delta\hat{X}'^2_4\rangle) \\
&= \tfrac{\eta(V+1)}{\alpha^2 T_{\min}}.
\end{aligned} \tag{A9}$$

Finally, we need to estimate the size of V_{NB}. Using the restrictions and simulation results we discussed in Section III, the worst strategy for Eve is choosing $\alpha^2 = \min(|\alpha'_s|^2, |\alpha'_{LO}|^2) = 10^3$, $T_{\min} = 0.1$ and $T_{\max} = 0.9$. Then $\frac{1}{\alpha^2(1-T_{\max})} = \frac{1}{\alpha^2 T_{\min}} = 10^{-2}$. Hence we get $V_{NB} < 10^{-2}\eta(V+1)$.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] B. Qi, C. -H. F. Fung, H. -K. Lo, and X. Ma, Quant. Inf. Comp. **7**, 7382 (2007).
[4] Y. Zhao, C. -H. F. Fung, B. Qi, C. Chen, and H. -K. Lo, Phys. Rev. A **78**, 042333 (2008).
[5] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Optics Express. **8**, 27938-27954 (2010).
[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics. **4**, 686-689 (2010).
[7] F. -H. Xu, B. Qi, and H. -K. Lo, New J.Phys. **12**, 113026 (2010).
[8] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature Comm. **2**, 349 (2011).
[9] C .Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).
[10] H. Weier, H. Krauss, M. Rau, M. Füerst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).
[11] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501(2011).
[12] S. -H. Sun, M. -S. Jiang, and L. -M. Liang, Phys. Rev. A. **83**, 062331 (2011)
[13] H. -W. Li, S. Wang, J. -Z. Huang, W. Chen, Z. -Q. Yin, F. -Y. Li, Z. Zhou, D. Liu, Y. Zhang, G. -C. Guo, W. -S. Bao, and Z. -F. Han, Phys. Rev. A. **84**, 062308 (2011).
[14] S. -H. Sun, M. Gao, M. -S. Jiang, C. -Y. Li, and L. -M. Liang, Phys. Rev. A. **85**, 032304 (2012)
[15] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[16] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, arXiv:1210.6216 (2012).
[17] http://www.sequrenet.com/
[18] http://qlabsusa.com/
[19] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature. **421**, 238 (2003).
[20] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004); C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. A. **73**, 022316 (2006).
[21] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, P. Grangier, Phys. Rev. A. **72**, 050303 (2005).
[22] H. Häseler, T. Moroder and N. Lütkenhaus, Phy. Rev. A. **77**, 032303 (2008).
[23] F. Grosshans, N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
[24] J. Lodewyck, and P. Grangier, Phys. Rev. A. **76**, 022332 (2007); J. Sudjana, L. Magnin, R. García-Patrón, and N. J. Cerf, Phys. Rev. A. **76**, 052301 (2007).
[25] M. Eisenmann, and E. Weidel, J. Lightwave Tech. **6**, 8588-8594 (2010).
[26] A. Ankiewicz, A. Snyder and X. -H. Zheng, J. Lightwave Tech. **4(9)**, pp1317-1323 (1986).
[27] V. Tekippe, Fiber and Integrated Optics. **9(2)**, 97-123 (1990).
[28] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[29] S. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[30] H. Bachor and T. C. Ralph, "A Guide to Experiments in Quantum Optics", 2nd Edition, WILEY-VCH Press (2003).

[31] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[32] R. García-Patrón, Ph.D. thesis (Université Libre de Bruxelles) (2007).